Electronic Signatures

Multi-state reciprocity

presented by:

Office of the Secretary of State

Michael Totherow, Chief Information Officer

Russ Savage, Electronic Transactions Liaison

So what's the Problem?

- E-SIGN requires technology neutrality while we have to implement something using specific technology
- We as states need to agree on what is readable, permanent "paper" and "indelible ink"

What's the Solution?

- *A technology neutral framework (a set of rules)*
- *A bridge from the general rules to rules for the general use of specific technologies*
- *We can then implement something using the agreed technology specific framework(s).*

Potential Pitfalls

- E-Sign & UETA ambiguous on Technology
  - If no technology specification, how much detail?
  - Multiple solutions popping up
    - based on un-tested technology
  - No specifics in law leads to Courts charting course
- State Signature Law guides Agencies, but
  - Digital Signature Technology is expensive
  - Infrastructure does not exist
  - Pending questions in lean times, is it cost effective?

Focusing on an E-Signature Future

- Secretary of State focusing on
  - responsibility for rules and procedures by law
  - maintaining technology agnostic approach
  - ensuring legal backing
  - participating with national and multi-state efforts
- Ultimate goal is key:

Interoperability

Interoperability - WHY?

We understand paper and ink, and
we have standards - 8 1/2 x 11 inches, "permanent" ink, etc.

We have open questions:

How do we "read" electronic documents filed with us by the private sector or by other jurisdictions?

How do we store, retrieve and forward those documents?

How do we know the next jurisdiction will accept them?

E-SIGN related multi-state Initiatives

August 10 & 11, 2000 - California Secretary of State sponsored a *Multi-State Digital Signature Summit* "in an effort to pool the collective expertise of state policy executives and technology experts and identify ways to remove barriers to the implementation of digital signature technology."

Discussion about E-SIGN at that meeting lead to -

Sept 6, 2000 - National Governors' Association (NGA) hosts meeting regarding state issues relating to implementation of the federal Electronic Signatures in Global and National Commerce Act (E-SIGN). Focused on prospective preemption of state laws, interoperability among states and retention requirements for state agencies.

That meeting led to NECCC being charged with coordinating four *E-SIGN forums: Legal, Policy, Security/Privacy, and Interoperability*.

E-SIGN related multi-state Initiatives

- "The primary effect of E-SIGN should be on private entities that wish to use electronic signatures and electronic records as they conduct business. States should only be affected in so far as their activities must recognize and accommodate the use of electronic signatures and electronic records in the private sector."
- "Another area where states should be prepared to deal with electronic signatures and documents is in their use in court. Although specific court documents, such as briefs, are exempted from E-SIGN, electronic contracts admitted as evidence are not."

What Governors Need to Know About E-SIGN:
The Federal Law Authorizing Electronic Signatures and Records,
NGA whitepaper, August 1, 2000

States will need to be prepared to accept private entity documents as evidence in courts and by any state agencies regulating those entities, *including private entity documents originally created for another state.*

E-SIGN related multi-state Initiatives

E-SIGN Interoperability forum

Vision Statement

December 2000

E-SIGN: "Electronic Signatures in Global and National Commerce Act."

"Using electronic signatures means creating signed electronic documents. This forum will begin by asking 'how do we get from technology neutral e-signatures statutes to agreement about what are sharable, trustworthy signed electronic documents (things that are reliable, usable, authentic, and having integrity)?'"

E-SIGN Forums met for a day and a half before the NECCC annual conference in December, 2000.

E-SIGN related multi-state Initiatives

The Interoperability forum defined the essential requirements for a formally formed electronic signature as follows:

Secure electronic signatures

A signature is a secure electronic signature if, through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:

- Unique to the person using it.
- Capable of verification.
- Under the sole control of the person using it.
- Linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

E-SIGN related multi-state Initiatives

The Interoperability forum defined the essential requirements for a formally formed electronic record as follows:

Secure electronic records

If, through the ongoing application of a security procedure, it can be demonstrated that an electronic record signed by a secure electronic signature has remained unaltered since a specified time, the record is a secure electronic record from that time of signing forward.

The Interoperability forum recognized that there are many processes to form these signatures and documents. And that there are varying levels of certainty desired for identifying a person, attributing a signature to them and assuring the integrity of the signed document.

The next step was to define a technology neutral **Framework for Electronic Signature Reciprocity** that identifies appropriate implementations for basic, medium, and high trust levels as far as how the:

- Signer is identified.
- Signer is linked to the signature.
- Signature is linked to the integrity of the record.

E-SIGN related multi-state Initiatives

The Interoperability forum now has four task teams working on:

1. developing a Model Certificate Policy (PKI) that is geared toward the needs of states as defined by the Framework for Electronic Signature Reciprocity.
2. drafting recommended elements for XML signing practices that various groups can use as they form their particular set of defined XML records.
3. drafting a Policy Management Authority white paper which will present the case for state's using a central authority model to manage signing processes (similar to Arizona's Policy Authority).
4. addressing the issues of electronic notary and electronic copy certification with the hope of working toward a framework for e-notary reciprocity.

The Value of Framework for Electronic Signature Reciprocity

The Interoperability forum's *Framework for Electronic Signature Reciprocity* provides a basic structure for states and state agencies to build technology specific processes that can be evaluated and accepted by other states much as we have inter-governmental agreements now. The model Certificate Policy will then lead to more direct interoperability of PKI processes. In fact there is an indirect link between this forum and the Federal PKI efforts to assure interoperability between state and federal PKI systems.

The Framework also establishes minimum criteria for states to evaluate other forms of electronic signatures and records and reach agreements on what will be recognized between states as acceptable processes.

This establishes a common definition among states of electronic "paper" and electronic "pen and ink" as well as electronic "signature."

E-SIGN related multi-state Initiatives

Common Certificate Policy provides Interoperability among States

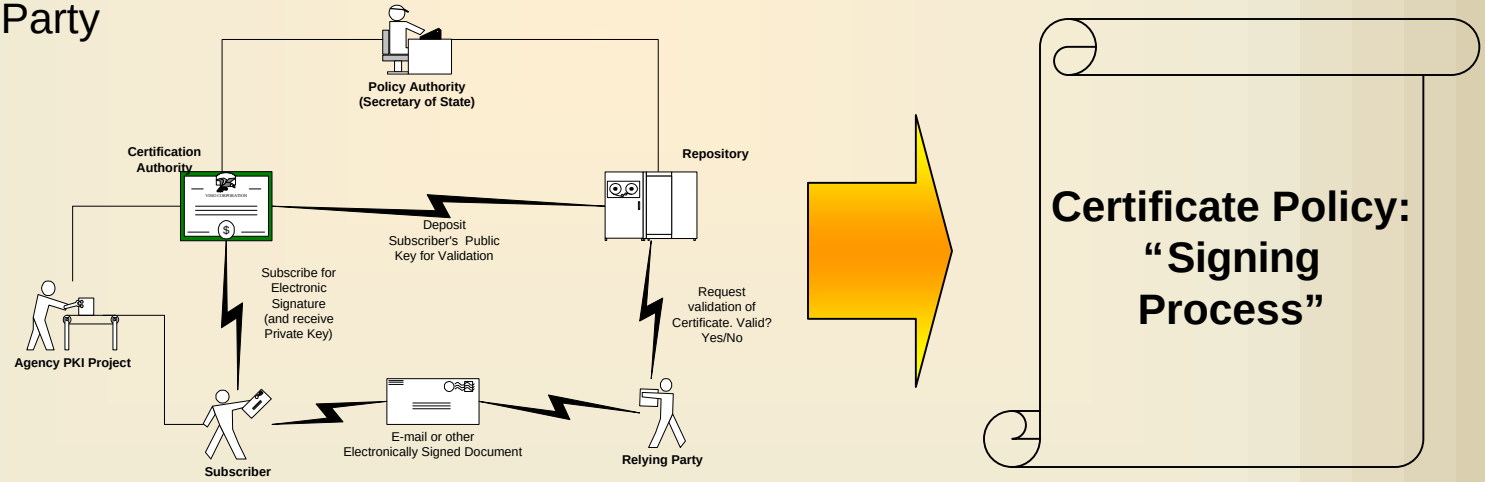
Our active participation in developing the model Certificate Policy will lead to more direct interoperability of PKI processes. In fact there is an indirect link between this forum and the Federal PKI efforts to assure interoperability between state and federal PKI systems.

The Framework also establishes minimum criteria for states to evaluate other forms of electronic signatures and records and reach agreements on what will be recognized between states as acceptable processes.

The entire process is setup so that any community of interest can adopt the framework and “drill down” to the specific tools they need with some assurance that their signing process will fit within a multi-state system of use.

The Structure of Electronic Signatures Arizona

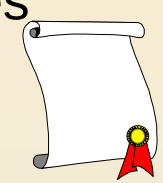
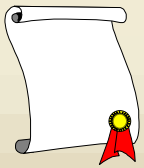
- Based on ‘Digital Signature’ roles and responsibility
  - Policy
  - Issuance of Technology
  - Subscriber Party
  - Repository Control for access & maintenance
  - Relying Party



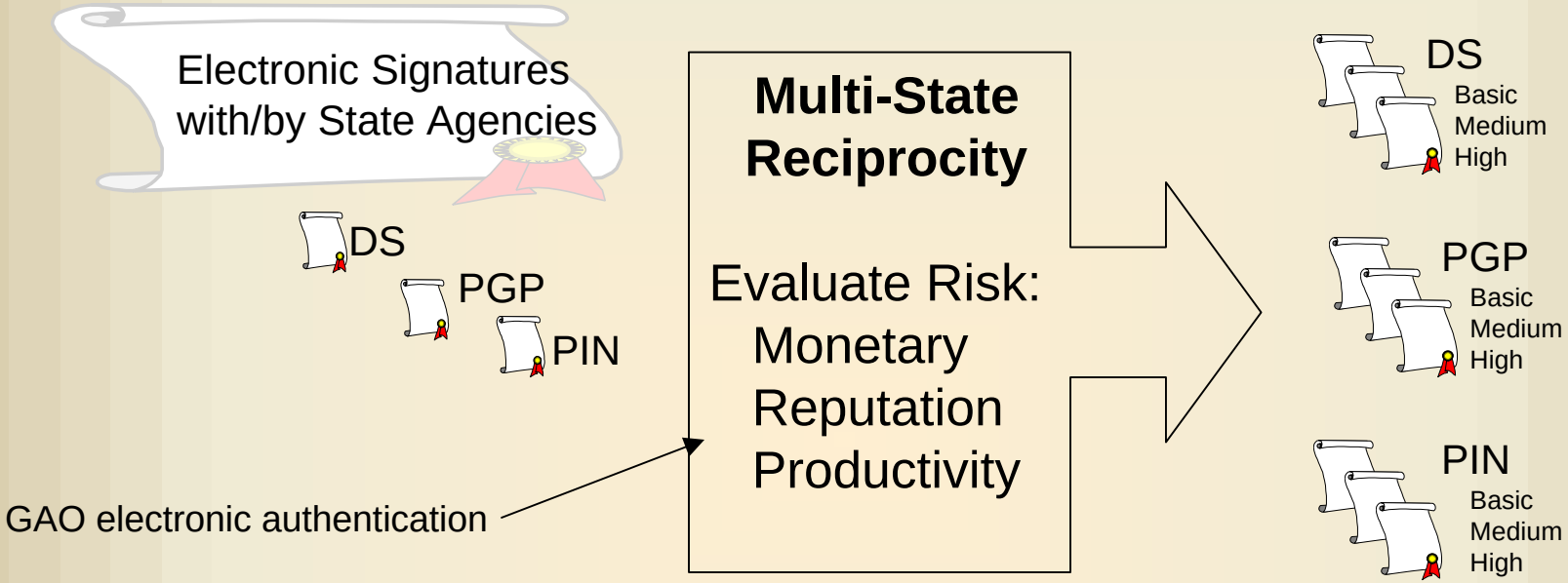
- Don’t confuse ‘Certificate Policy’ with *Digital Signature* technology - focus on the word “policy”

Maintaining Interoperability by Policy

- Structure of Infrastructure
  - Electronic Signatures
    - (41-132 - unique to person; reliable verification; linked to record)
    - Rule
      - governing “electronic signing process”
      - developing Policy
      - identifying technology
      - Acceptable Technologies
        - Digital Signatures
        - Pretty Good Privacy (pending)
        - Personal Identification Numbers (pending)


Creating something of Infra “Structure”



The “Certificate Policy” is the “Contract and Specification”

Operating Parameters

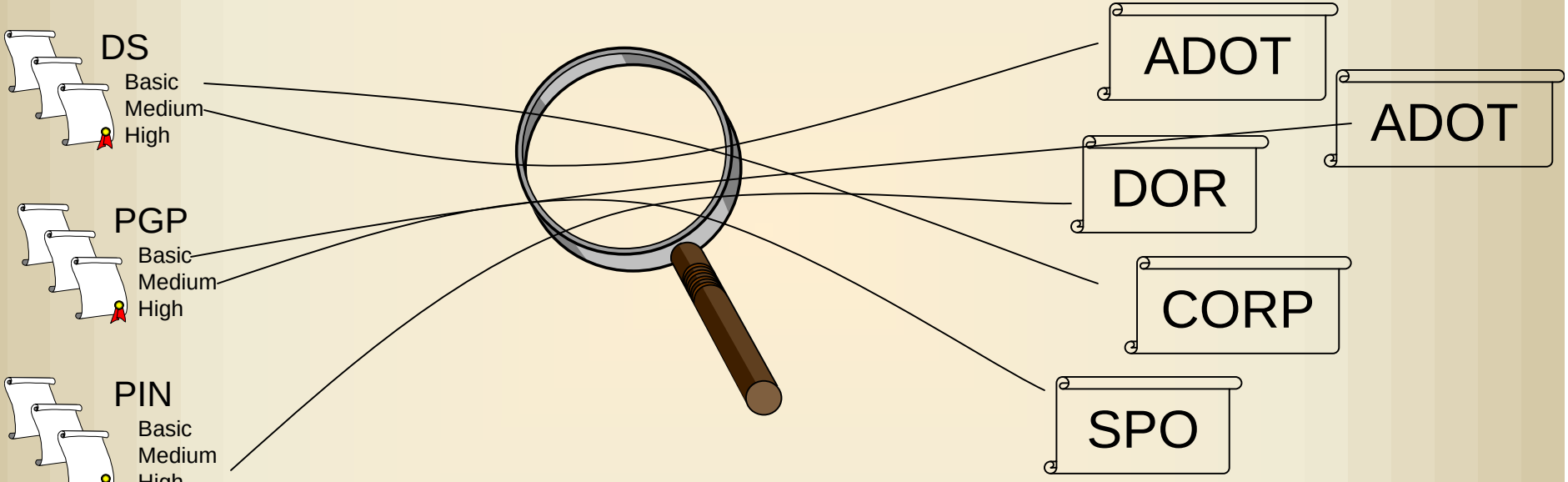
Roles & Responsibilities

Boiler Plate Language

Used to bridge the technologies amongst jurisdictions

Interoperability is a map

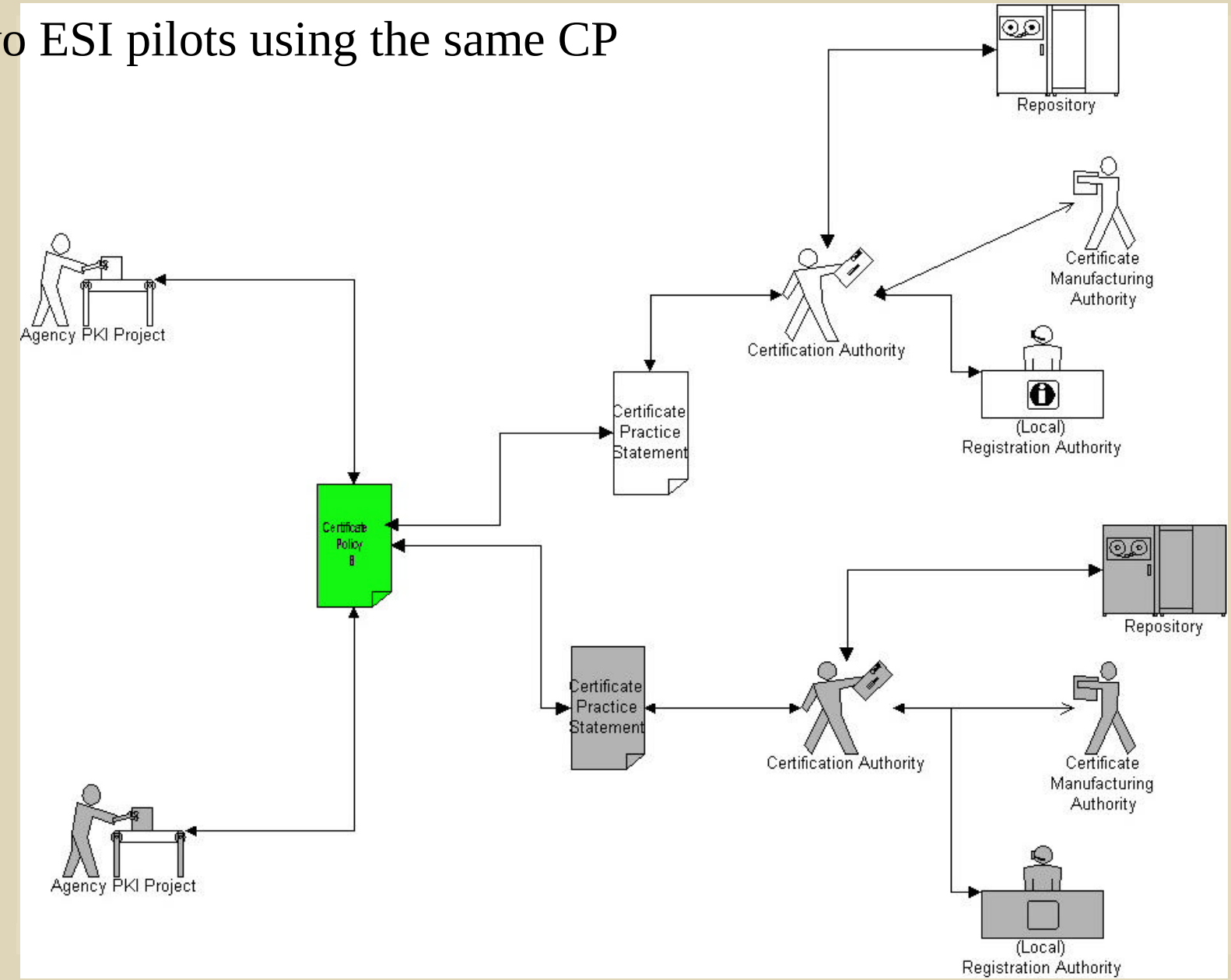
Secretary of State becomes the focal point of mapping the "Signing Process" in the State

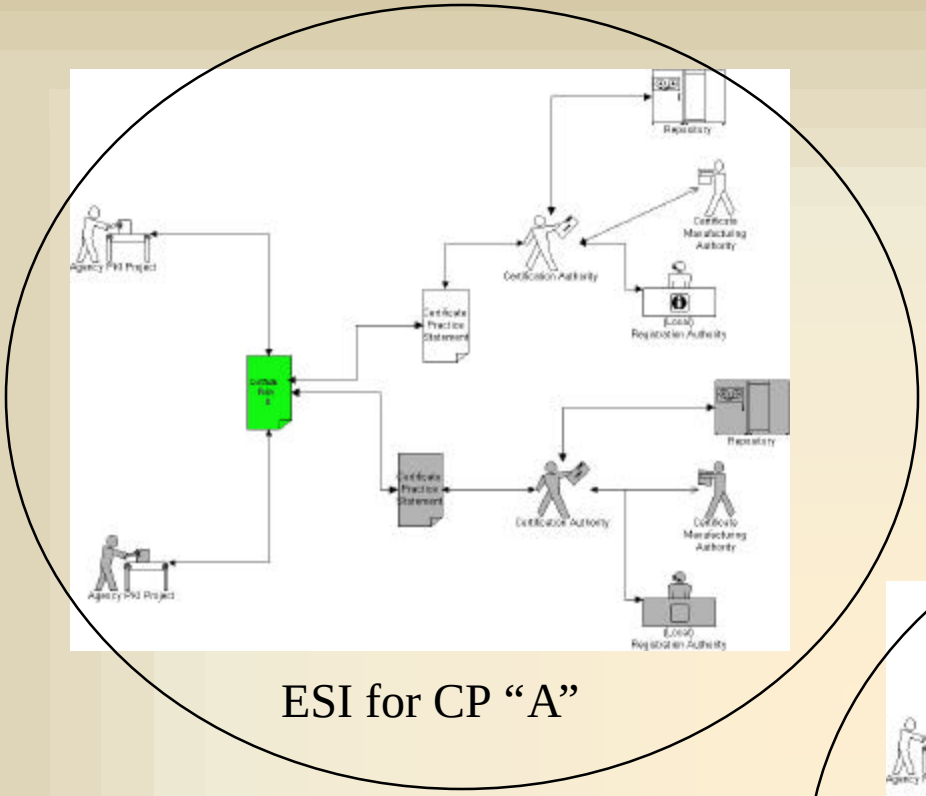


Communities of Interest resolve to a "CP"…

- Communities may not "rely" on other communities
- Communities could "traverse" the map
- Interoperability is at least "policy level"

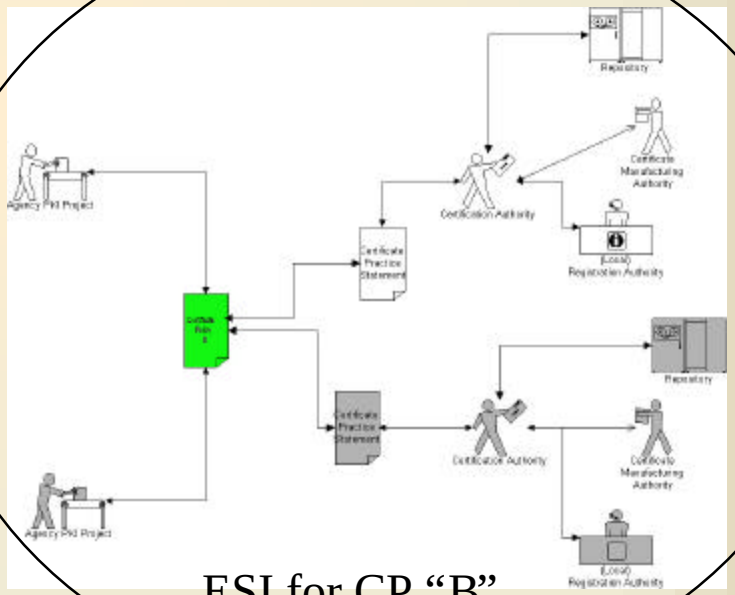
Two ESI pilots using the same CP



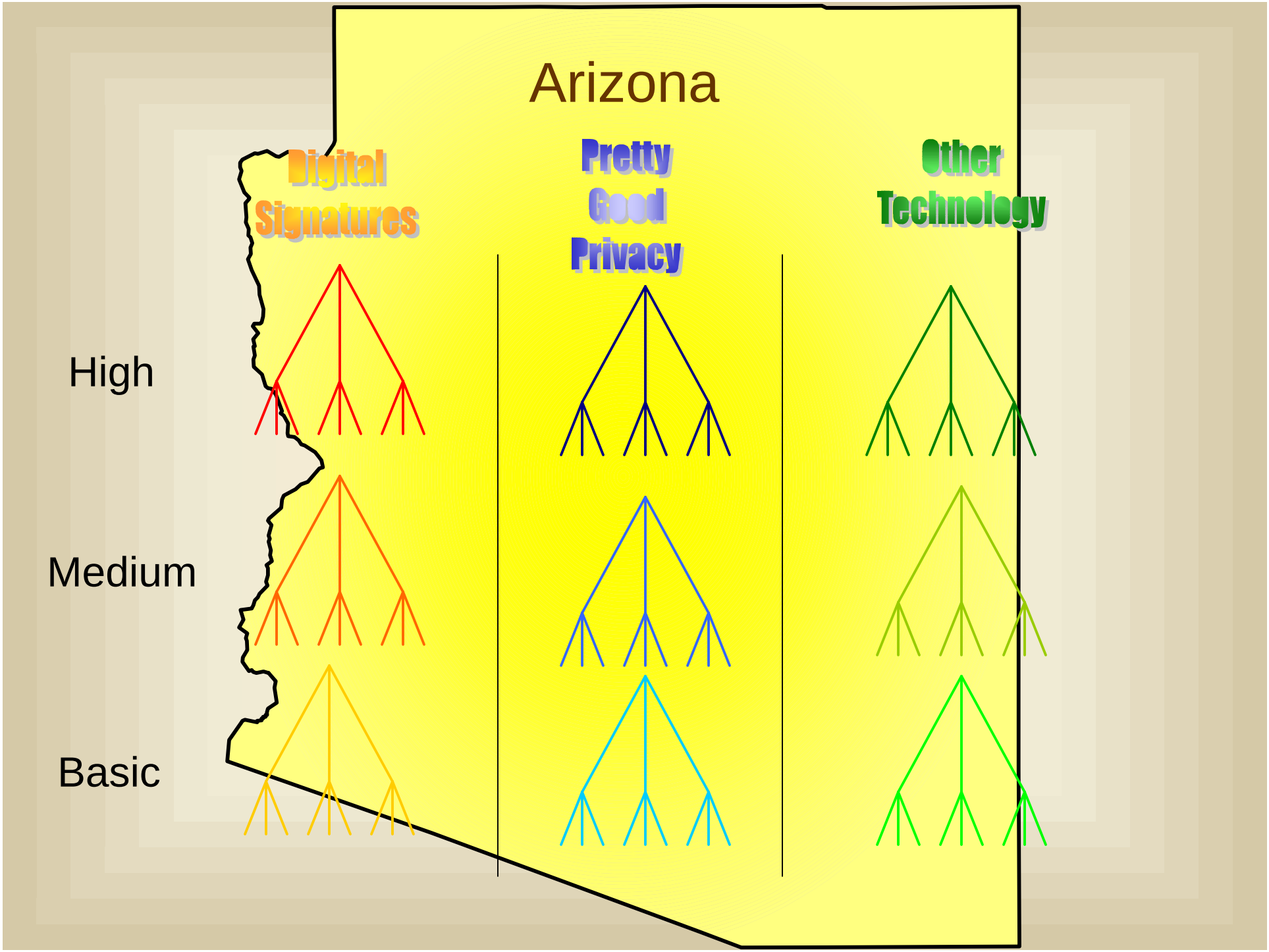


ESI for CP “A”

The AESI consists of several collections of pilots (ESIs) organized around different Certificate Policies (CPs).



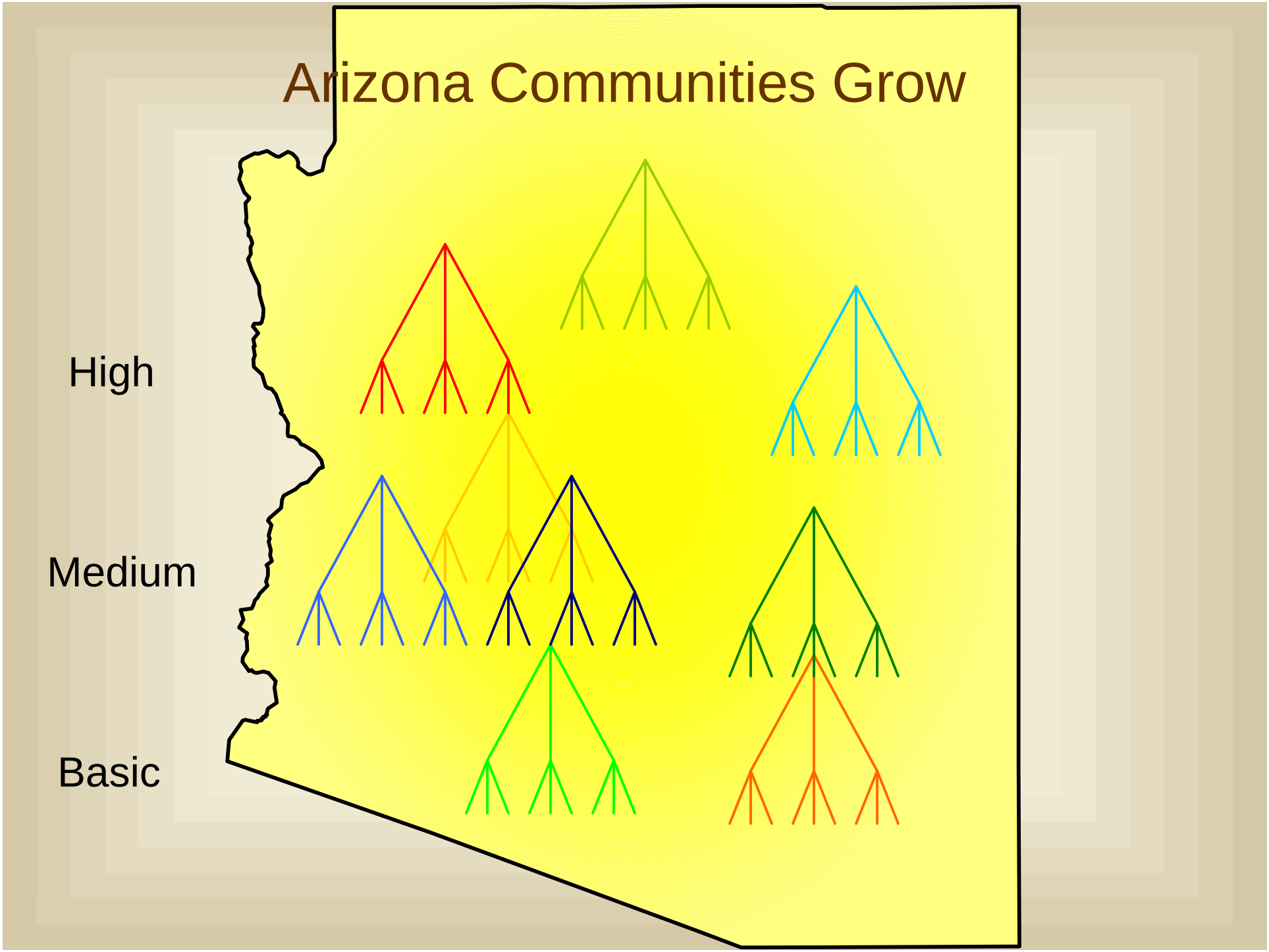
ESI for CP “B”


Arizona
Digital Signatures
Pretty Good Privacy
Other Technology
High
Medium
Basic

Communities of Interest

- Based on interest, not jurisdiction
- Need within community for electronic signing
  - Reduce time constraints
  - Reduce location restraints
  - Automate the operation of the Community
- Jurisdictions serving community
  - Must be interested in participation
  - Resources for participation
  - Willing to collaborate with other jurisdictions
  - Agree to level of assurance required for community enrollment

Arizona Communities Grow



Reliance (Community Evidence)

- Within the community
  - agreement of community enrollment
  - agreement of jurisdictions governing community
  - common understanding of evidence
- Outside the community
  - What are you missing?
    - Who else relies upon evidence created in community
    - What other jurisdictions must the evidence be presented
    - How will the evidence be communicated
      - Tool set / application “exportable”
    - How will evidence be proven
      - Self evidencing documentation
      - Jurisdiction (perhaps community wide) system security

Clear Examples of cross jurisdiction

- Common interest, but multiple X multiple jurisdictions and reliance
  - Procurement
  - Healthcare
- Common interest with one jurisdiction with multiple X multiple reliance
  - Electronic Notary
  - Copy Certification

- Electronic Notary can be the bridge of multi-jurisdictional reliance and communication

What is a "signature"?

Consider the reasons to use a secure electronic signature (the "legal" reasons for a formal signature - wet or electronic):

1. to identify the person signing (the identification function);

2. to indicate that person's approval of the information contained in that data message (the authentication function);

3. to indicate that the record has not been altered (the integrity function).

Notarization accomplishes these -

even if the person only makes their mark.

Electronic Signatures Framework for multi-state Interoperability

- fully self-documented electronic record (e.g. PKI/XML)
  (evidence based on test of record)
- fully trustworthy record/document system (e.g. EDI)
  does not have self-documented electronic records
  (evidence based on testimony about the system)
- fully self-documented electronic record *in*
  a fully trustworthy document system (e.g. PKI/XML/EDI)
- fully trustworthy record/document system
  does not have self-documented electronic records *but*
  can reliably export a self-documented electronic record
  (e.g. From EDI to PKI/XML)

Notarization or certified copy can bridge incompatible document systems.

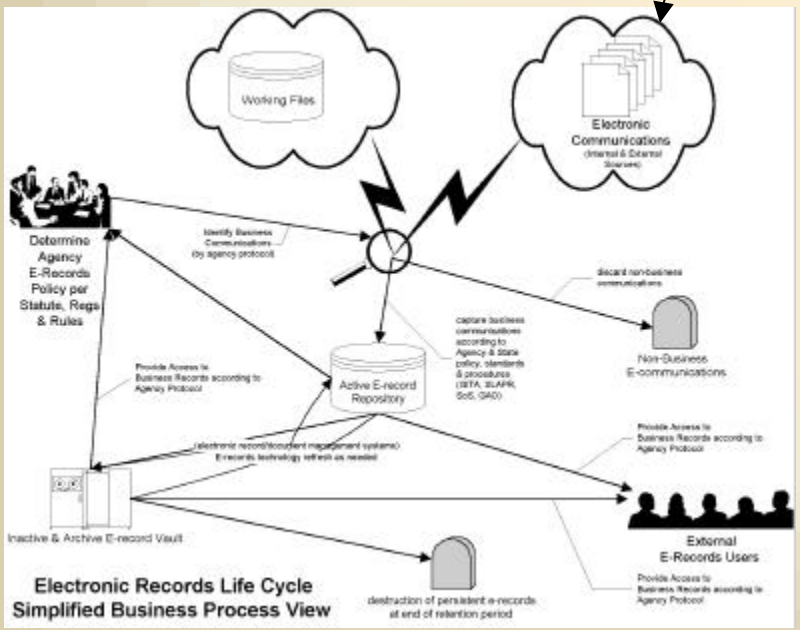
Electronic Signatures Framework for multi-state Interoperability

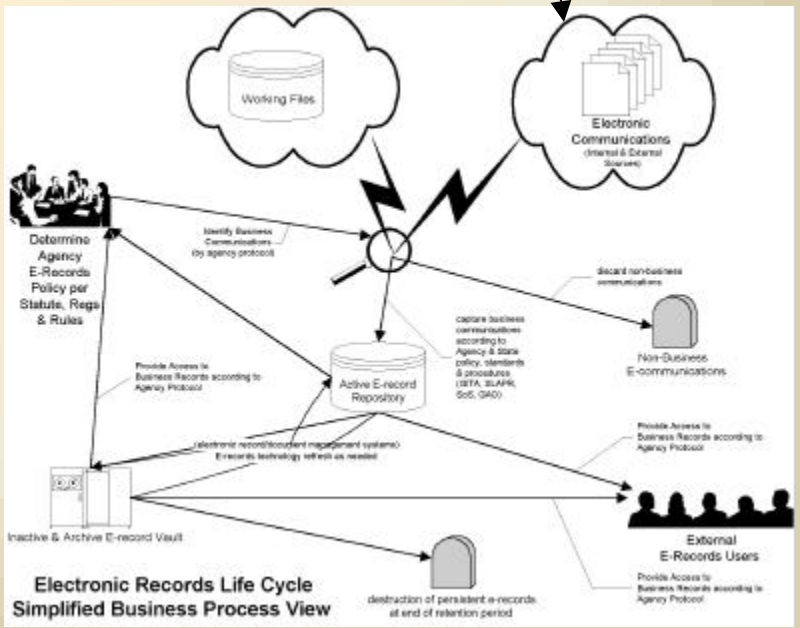
Why the fuss about e-signature & e-documents?

Because some of mine will migrate to your place and some of yours will migrate to my place. They need to be readable and they need to be verifiable.

Notarization or “certified copy” can do that between incompatible document systems.

Interoperability
getting from here to over there





Electronic Signatures Framework for multi-state Interoperability

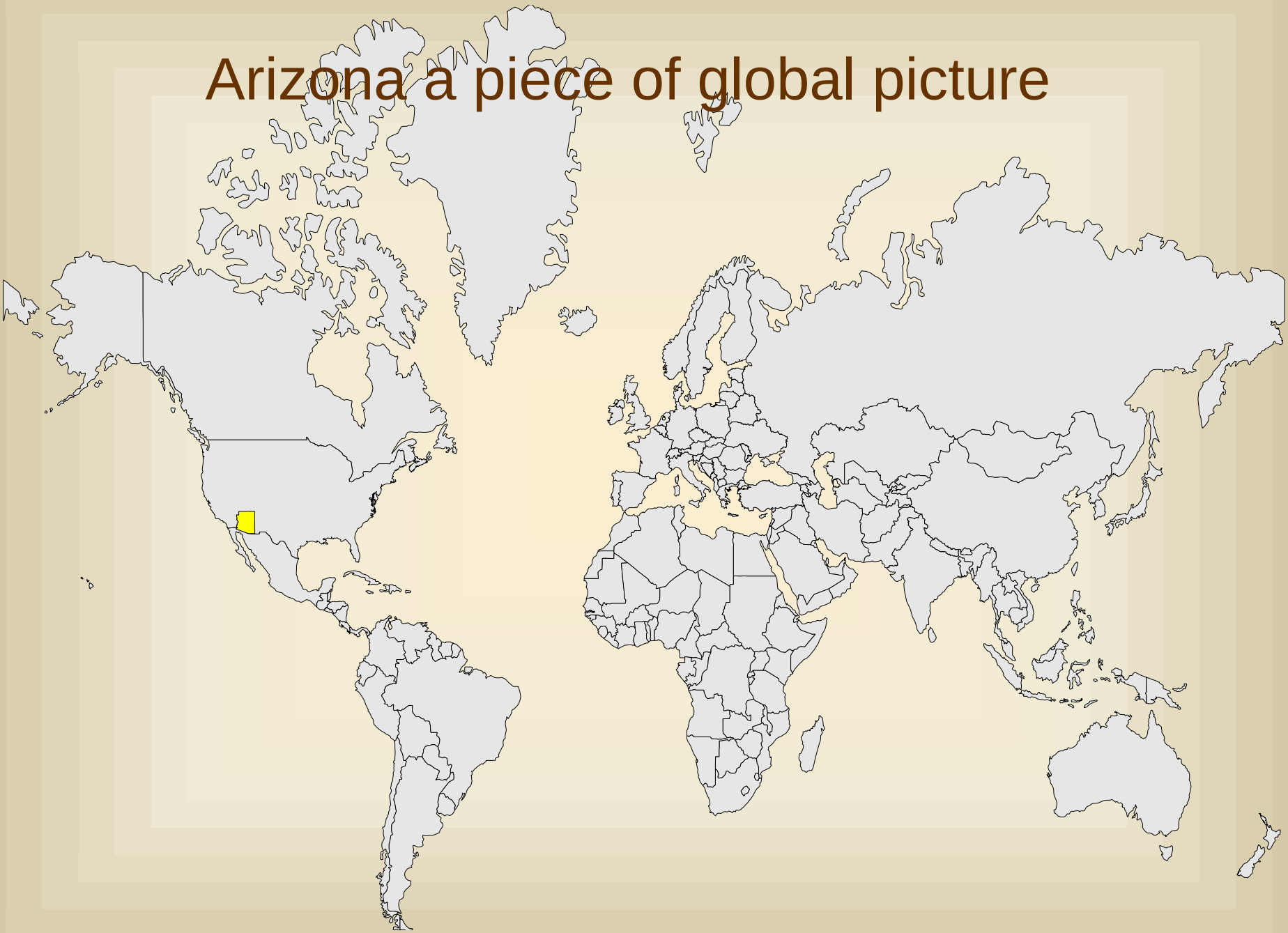
Summary

Multi-state reciprocity on electronic notary can reduce the complexity of other interoperability issues by allowing generalized cross-jurisdiction “copy certification” of non-self-documenting records.

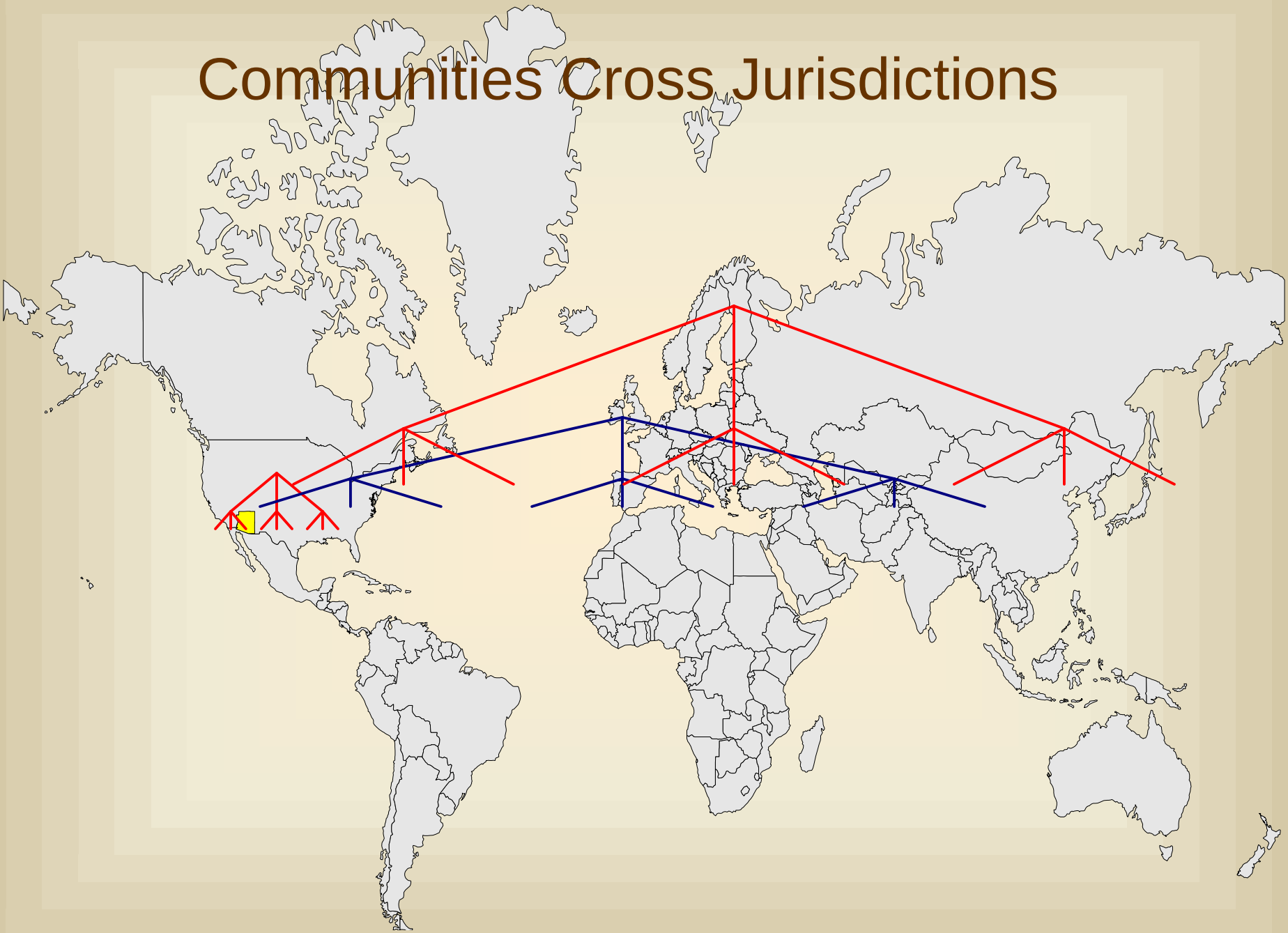
Arriving at electronic notary reciprocity will address nearly every interoperability issue. The solutions found for it can form the basis for general principles in other interoperability situations.

Any issues not addressed will likely surface in the HIPAA and e-mall/e-procurement processes that the E-SIGN Interoperability forum will explore this year.

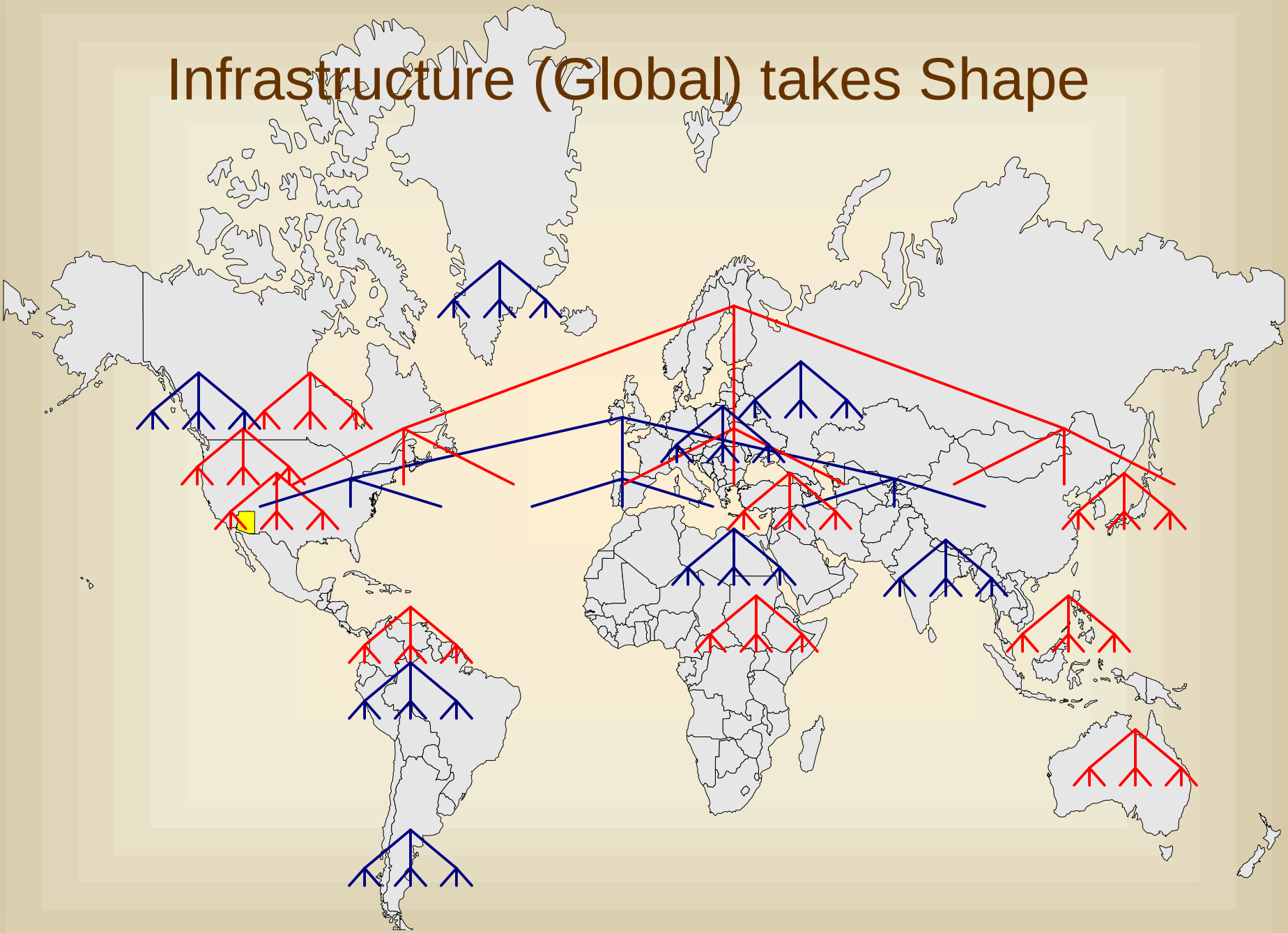
Arizona a piece of global picture



Communities Cross Jurisdictions



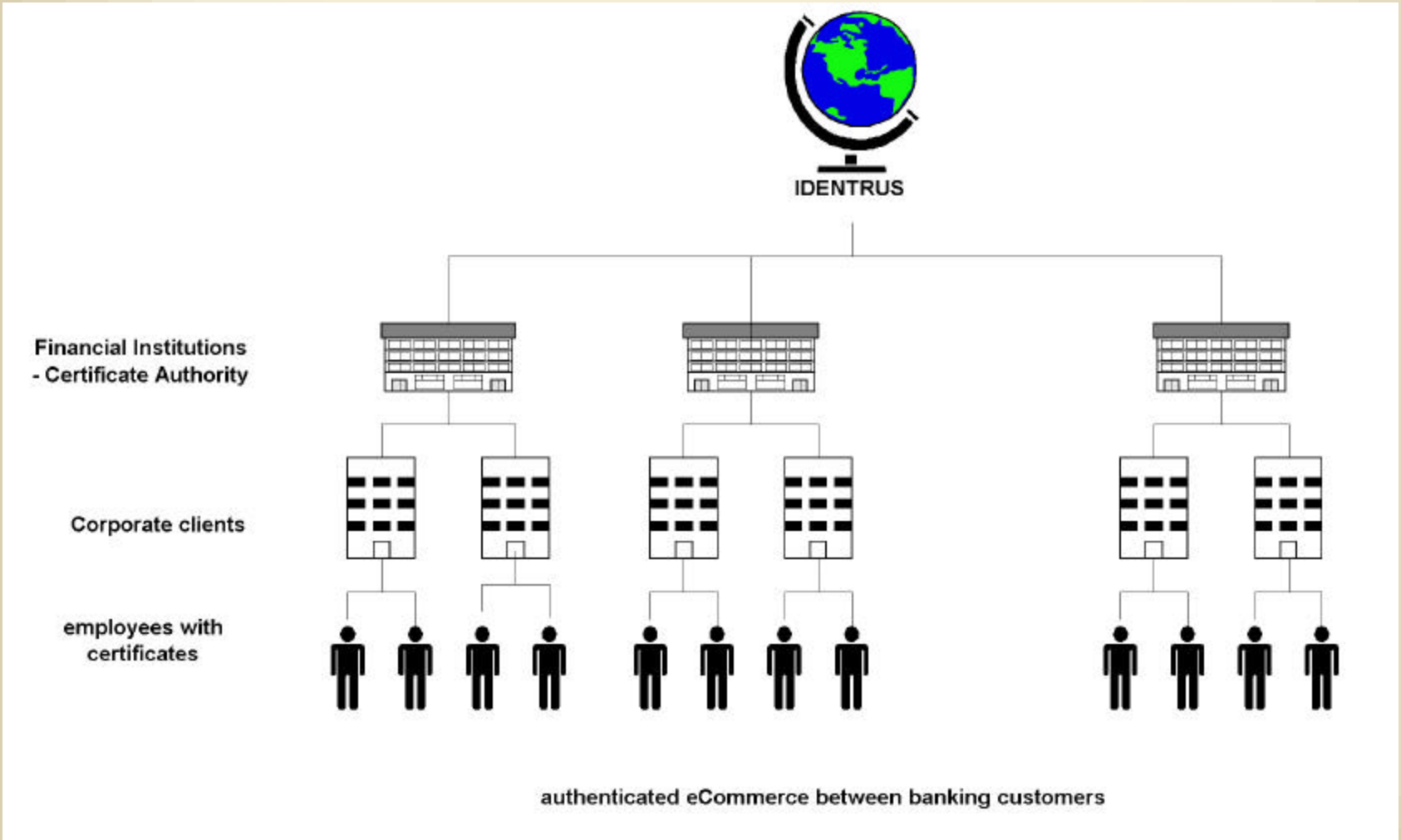
Infrastructure (Global) takes Shape



E-transactions: Ingredients, Recipe, Season-to-Taste

Identrus

an international banking trust initiative
via an interoperable PKI network



Movement begins with Understanding

- Education already taking place
  - Campaign Finance - electronic filing.
    - Because the elected officials ultimately are those that make the decisions about technology laws, so the campaign finance electronic reporting is preparing them for understanding the ease, and complexities, of dealing with electronic signatures.
- Education in the works
  - Lobbyist reporting.
    - Like the elected officials, educating the “persuaders” of the laws will help create smart laws.
  - Travel Reimbursement.
    - Aimed at the Directors, Supervisors and managers, to begin to educate them on electronic processes as they begin to investigate their own business practices moving to e-government.

What's happening in the State

- Certification Authorities applying for Approved Certification Authority list
  - waiting for business case before jumping through hoops
- State looking at internal processes for automation
  - Travel reimbursement
  - Procurement
  - Secured Access to Networks
- State building archive repository
  - Initial plans for archive only, investigating operations
    - eases exit strategy for agencies electronic record reliance
- State working with Multi-State efforts to develop common document exchange format
  - Levels of signing assurance
  - Electronic Notary
  - Standards for technology implementation
- State becomes repository of signing practices
  - best practices will emerge

What we need from you

- Begin with Process Re-thinking
  - We’re all novices at the e-gov game
  - No definite leaders… think elimination of red tape
    - Review needs for ‘intent’
    - achieve objectives by using risk assessment
- Define Community of Interest
- Agree on a “signing process”
  - Point to a ‘Certificate Policy’ for Technology
  - Submit ‘signing process’ with Secretary of State
- Begin to build the Infrastructure
  - Mini PKI just part of larger PKI
  - Promotes Interoperability within state and abroad